AP EXPLICA: ¿Qué es el ransomware?

Por MICHAEL BALSAMO
Associated Press, 13 de mayo de 2017

LOS ANGELES (AP) — Numerosas computadoras en el mundo fueron bloqueadas y los archivos secuestrados para exigir rescate durante un ataque cibernético con fines de extorsión contra hospitales, compañías y agencias gubernamentales en decenas de países.

A continuación presentamos un vistazo a la forma en que funcionan los llamados "malware" y "ransomware" y qué puede hacer la gente si es víctima de un ataque de este tipo.

¿QUÉ ES EL MALWARE Y EL RANSOMWARE?

Malware es un término genérico que designa un programa informático perjudicial para la computadora de alguien, dijo el profesor John Villasenor de la Universidad de California, plantel Los Ángeles. Un ransomware es un tipo de malware que en esencia se apodera de una computadora e impide al usuario acceder a la información archivada si no se paga un rescate, agregó.

¿CÓMO INFECTA EL RANSOMWARE UNA COMPUTADORA?

En la mayoría de los casos, el programa informático infecta las computadoras mediante enlaces o archivos adjuntos que llegan a los usuarios en correos

electrónicos maliciosos conocidos como “phishing” (suplantación de identidad, en la que se adquiere información confidencial en forma fraudulenta).

“La recomendación tradicional es nunca hacer click en un enlace que venga en un correo electrónico”, dijo Jerome Segura, investigador de inteligencia contra programas maliciosos en Malwarebytes, una compañía con sede en San José que tiene disponible en el mercado un programa informático anti-ransomware.

“La idea es engañar a la víctima para que corra un fragmento de código malicioso”, apuntó.

El software por lo general está escondido dentro de los enlaces o archivos adjuntos en los correos electrónicos. Si el usuario hace click en el enlace o abre el documento adjunto, su computadora se infecta y el programa informático se apodera de la máquina.

¿CÓMO FUNCIONA EL RANSOMWARE?

“El ransomware, como su nombre en inglés indica, sirve para secuestrar archivos y pedir un rescate”, dijo Peter Reiher, profesor adjunto en la UCLA especializado en ciencias de la computación y seguridad cibernética. “El programa encuentra todos los archivos, los encripta y deja un mensaje. Quien desee descifrarlos tiene que pagar”.

El ransomware encripta la información en la computadora mediante una clave de codificación que sólo el autor del ataque conoce. Si el rescate no es pagado, a menudo la información se pierde para siempre.

¿CÓMO EVITAR ESTOS ATAQUES?

La primera medida es la cautela, según los expertos. Sin embargo, Villasenor dijo que “no existe solución perfecta” al problema.

Los usuarios deberían hacer con regularidad copias de su información e instalar las actualizaciones de seguridad en la computadora en cuanto sean puestas a disposición del público. Si se tienen respaldos actualizados ello permite restaurar los archivos perdidos sin tener que pagar rescate alguno.

El ataque cibernético del viernes aprovechó las vulnerabilidades en algunas versiones de Microsoft Windows.

Microsoft ha difundido parches informáticos para cubrir los huecos de seguridad, aunque no todos los usuarios han instalado esas actualizaciones.

___

Michael Balsamo está en Twitter como: https://twitter.com/MikeBalsamo1